Отчёт по лабораторной работе 3

Дискреционное разграничение прав в Linux. Два пользователя

Максимова Ксения НБИбд-02-18

Содержание

[Цель работы 1](#_Toc85148350)

[Задание 1](#_Toc85148351)

[Теоретическое введение 1](#_Toc85148352)

[Выполнение лабораторной работы 2](#_Toc85148353)

[Выводы 19](#_Toc85148354)

[Список литературы 19](#_Toc85148355)

# Цель работы

Получение практических навыков работы в консоли с атрибутами файлов для групп пользователей.

# Задание

Создать двух пользователей в ранее установленной оперционной системе на виртуальной машине, определить установленные права, разрешенные действия и минимальные права для совершения оперций

# Теоретическое введение

В операционной системе Linux есть много отличных функций безопасности, но она из самых важных - это система прав доступа к файлам. Linux в отличие от Windows, изначально проектировался как многопользовательская система, поэтому права доступа к файлам в linux продуманы очень хорошо [[1]](https://losst.ru/prava-dostupa-k-fajlam-v-linux) .

Права доступа к файду или директории можно изменить с помощью команды chmod. Атрибуты файла или каталога можно указать как буквами так и цифрами. Установить необходимые атрибуты можно для владельца файла (u), группы (g) или остальных пользователей (o) [[1]](https://losst.ru/prava-dostupa-k-fajlam-v-linux).

Права достуа к какому-либо объекту в системе обозначаются с помощью 10 символов, записанных в строчку [[2]](https://linuxrussia.com/terminal-chmod-chown.html).

1. Первый символ в строке обозначает тип данных
2. Следующие три символа обозначают права для владельца файла или директории
3. После - права для определенной группы пользователей
4. Последние четыре символа - права для остальных пользователей

Рассмотрим, какими правами может быть наделен файл или директория:

* r - read, то есть, право доступа на чтение файла или директории.
* w - write, то есть, право на изменение и удаление файла или директории.
* x - eXecute, то есть, право на запуск файла как программы или вход в директорию.

Таким образом, можно ограничить или расширить права на файл тех или иных пользователей

Права доступа для пользователей группы определяются второй триадой символов в строчке прав, как и любой другой пользователь или владелец, пользователь группы может получить права на чтение, изменение или удаление, а так же запуск файла [[3]](https://moodle.kstu.ru/pluginfile.php/318215/mod_resource/content/1/Теория_разграничение_прав_пользователи.pdf)

# Выполнение лабораторной работы

В установленной операционной системе создаем учётную запись пользователя guest с помощью команды useradd

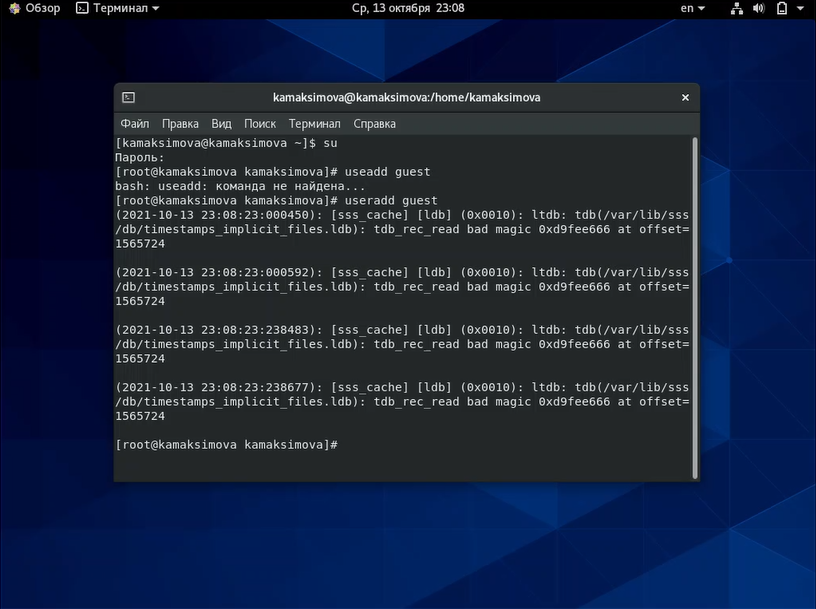


Рис 1.Создание нового пользователя

[Рисунок 1](image/Pic1.png)

Задаем пароль для пользователя guest с помощью команды passwd

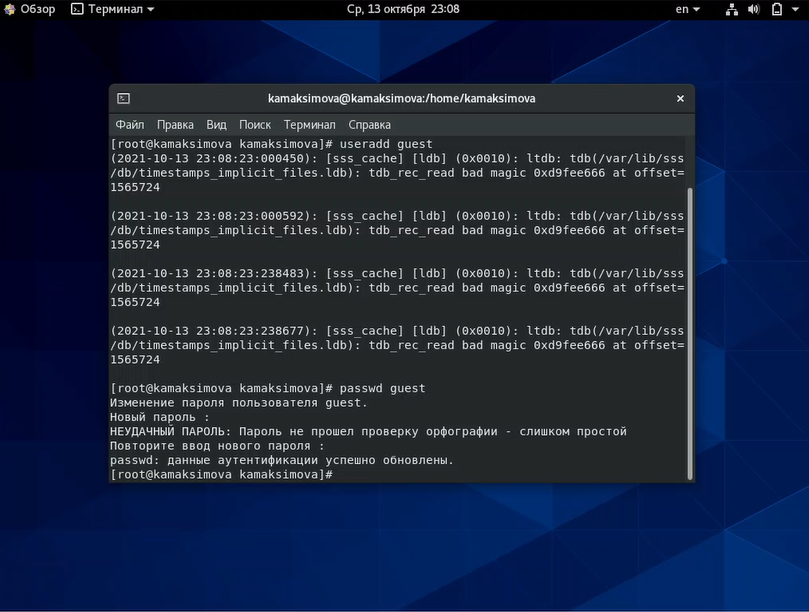


Рис 2.Установка пароля

[Рисунок 2](image/Pic2.png)

Аналогично создаем второго пользователя guest2

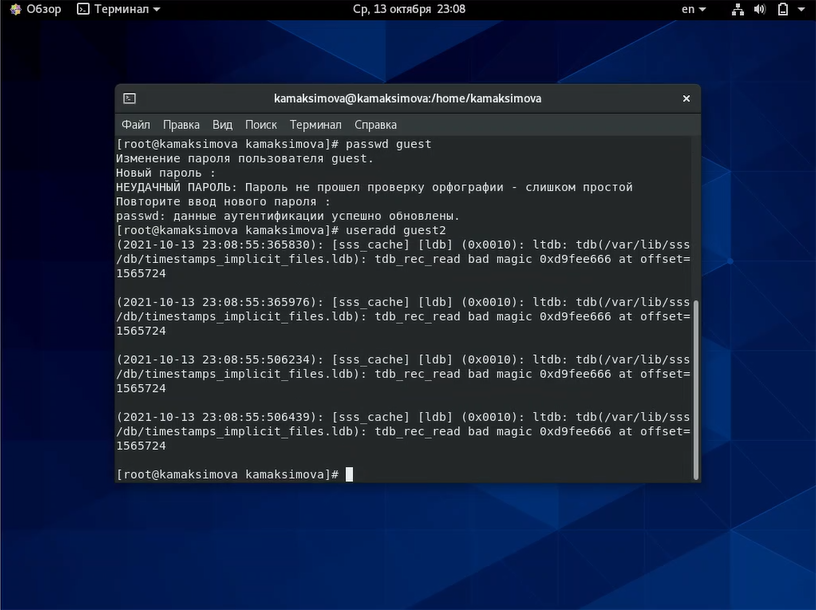


Рис 3.Создание пользователя guest2

[Рисунок 3](image/3.png)

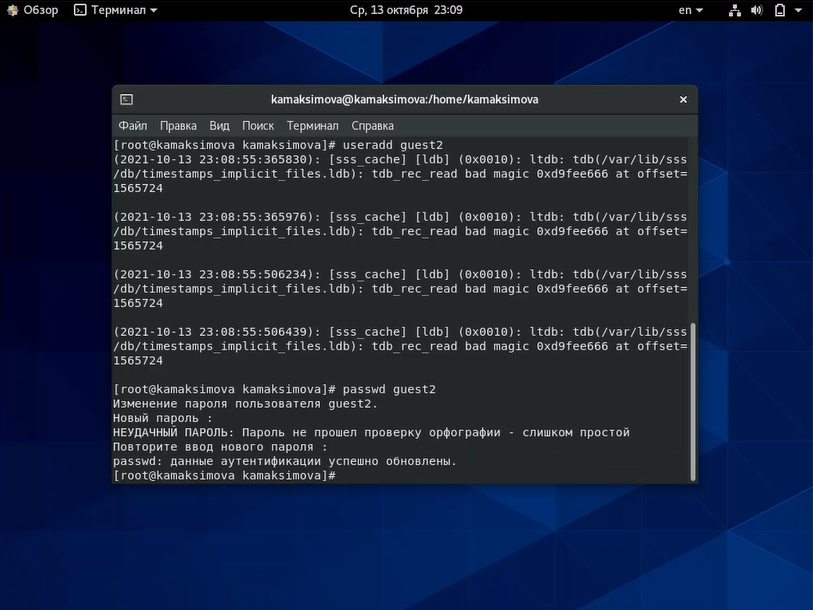


Рис 4.Задание пароля для пользователя guest2

[Рисунок 4](image/4.png)

Добавляем пользователя guest2 в группу guest

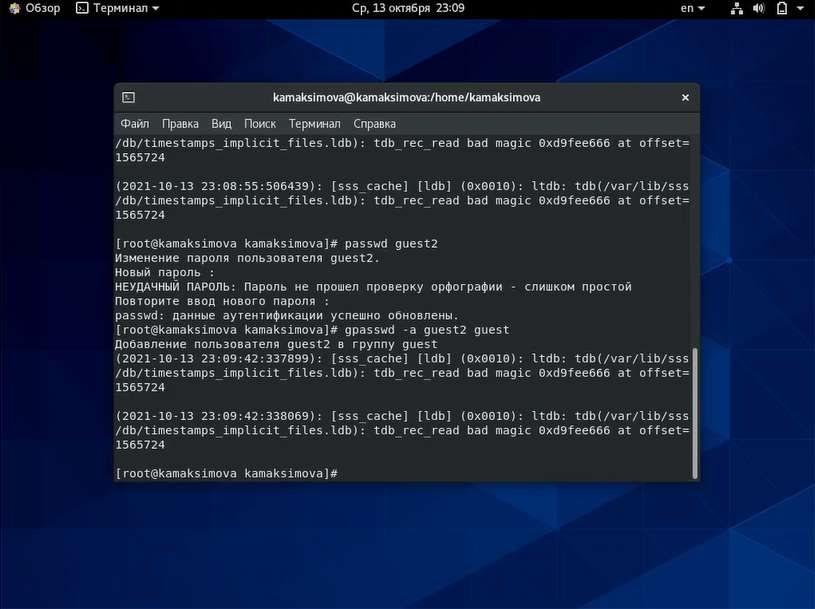


Рис 5.Добавляем пользователя guest2 в группу guest

[Рисунок 5](image/5.png)

Осуществляем вход в систему от двух пользователей на двух разных консолях: guest на первой консоли и guest2 на второй консоли

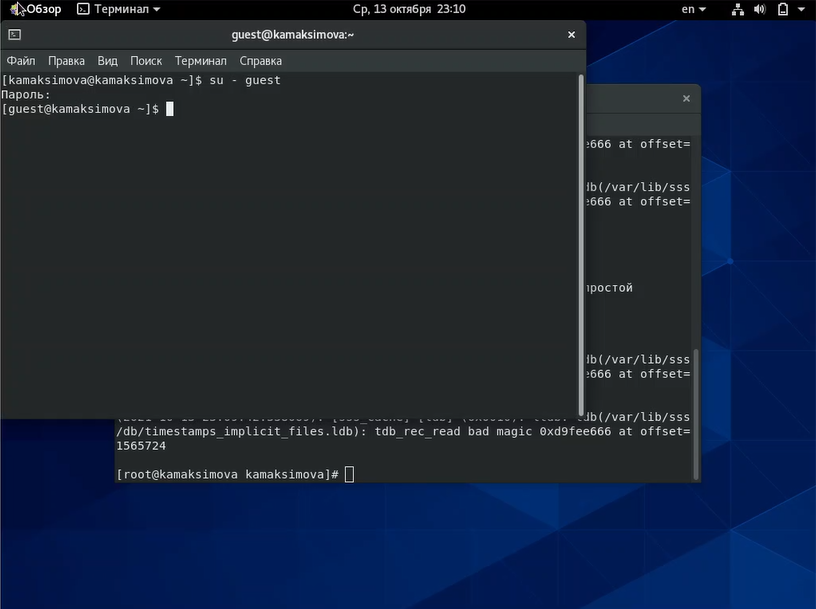


Рис 6.Осуществляем вход в систему от guest

[Рисунок 6](image/6.png)

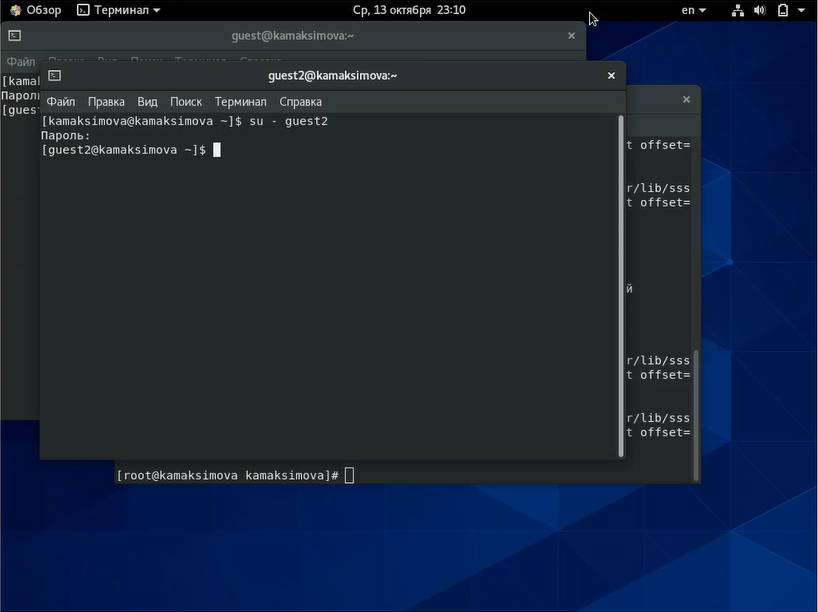


Рис 7.Осуществляем вход в систему от guest2

[Рисунок 7](image/7.png)

Для обоих пользователей командой pwd определяем директорию, в которой находимся

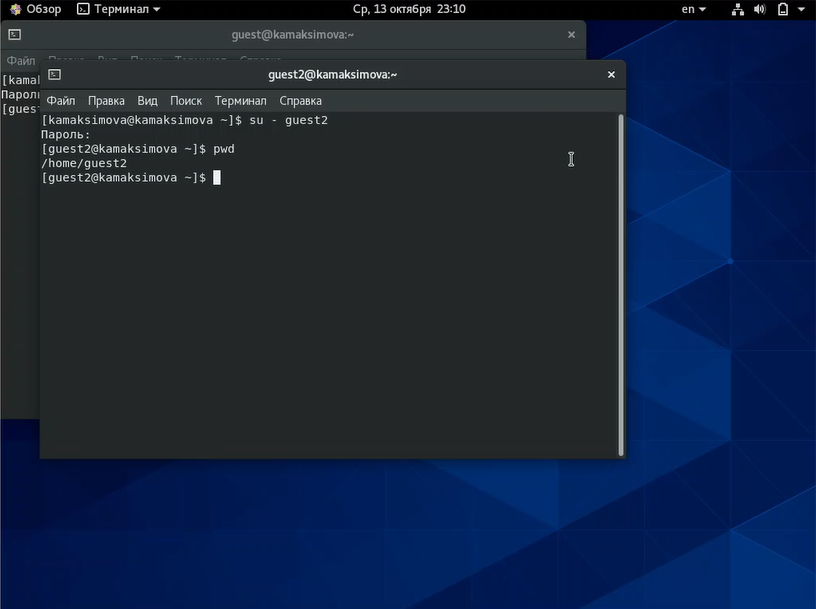


Рис 8./home/guest2

[Рисунок 8](image/8.png)

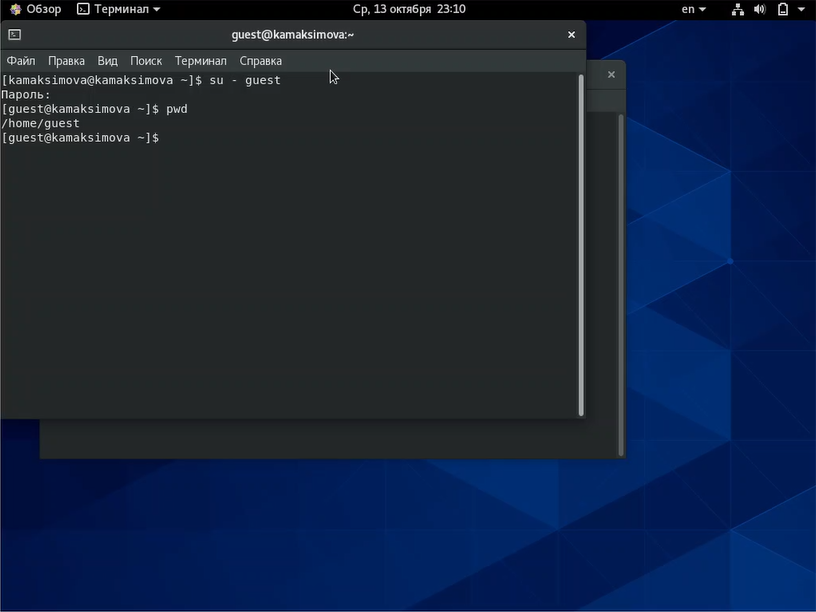


Рис 9./home/guest

[Рисунок 9](image/9.png)

Уточним имя пользователя, его группу, кто входит в неё и к каким группам принадлежит пользователь. Определим командами groups guest и groups guest2, в какие группы входят пользователи guest и guest2.

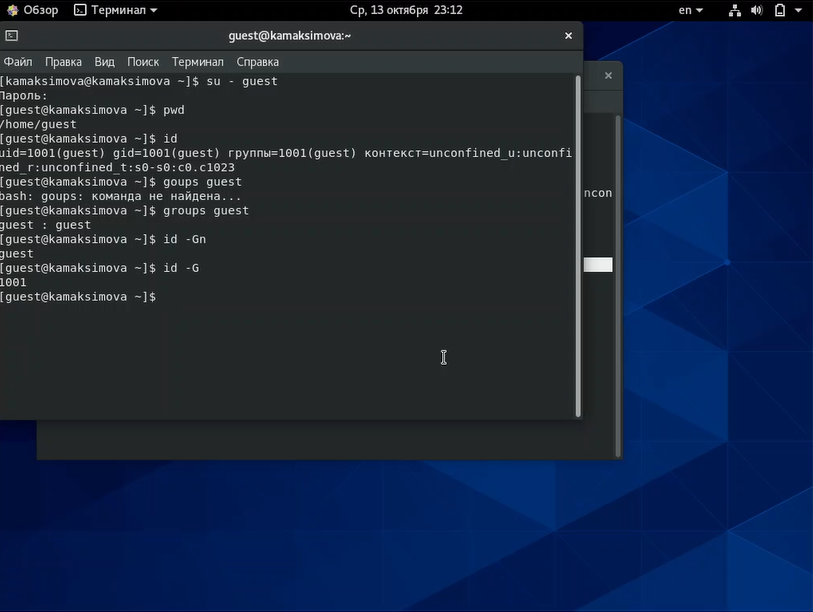


Рис 10.Команды id, groups guest, id -Gn и id -G для guest

[Рисунок 10](image/10.png)

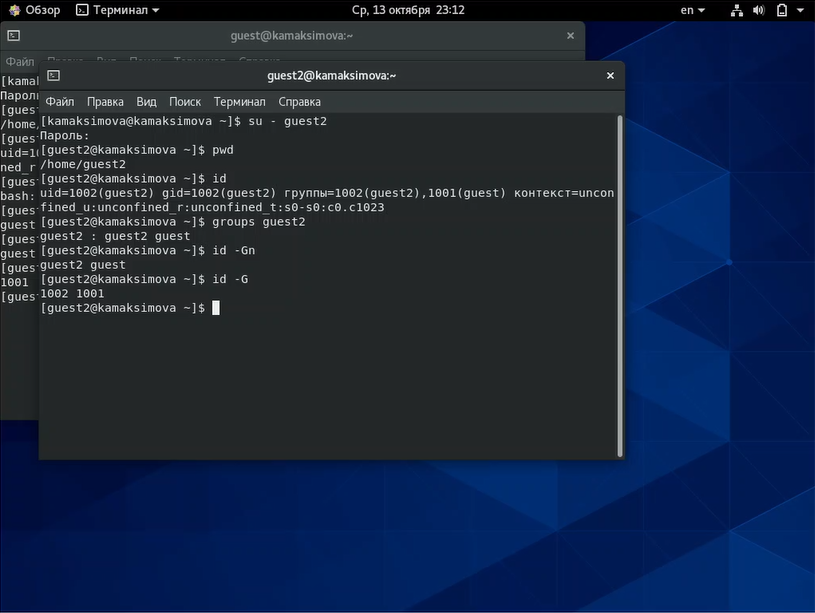


Рис 11.Команды id, groups guest, id -Gn и id -G для guest2

[Рисунок 11](image/11.png)

Просмотрим файл “/etc/group” командой cat

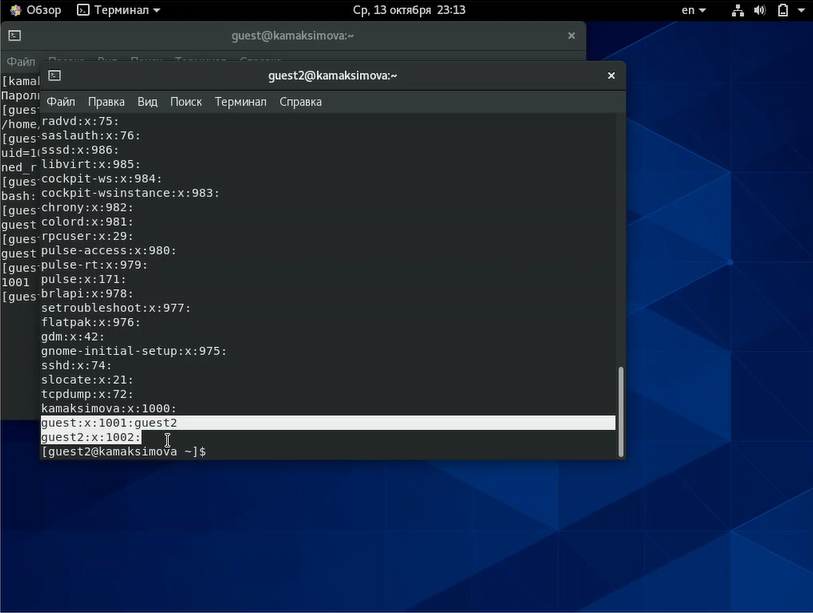


Рис 12. guest2

[Рисунок 12](image/12.png)

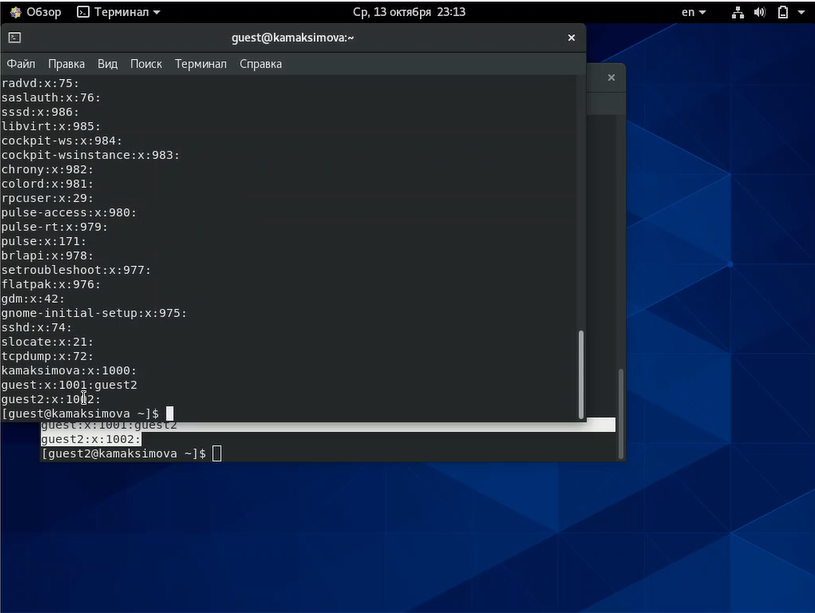


Рис 13. guest

[Рисунок 13](image/13.png)

От имени пользователя guest2 выполним регистрацию пользователя guest2 в группе guest

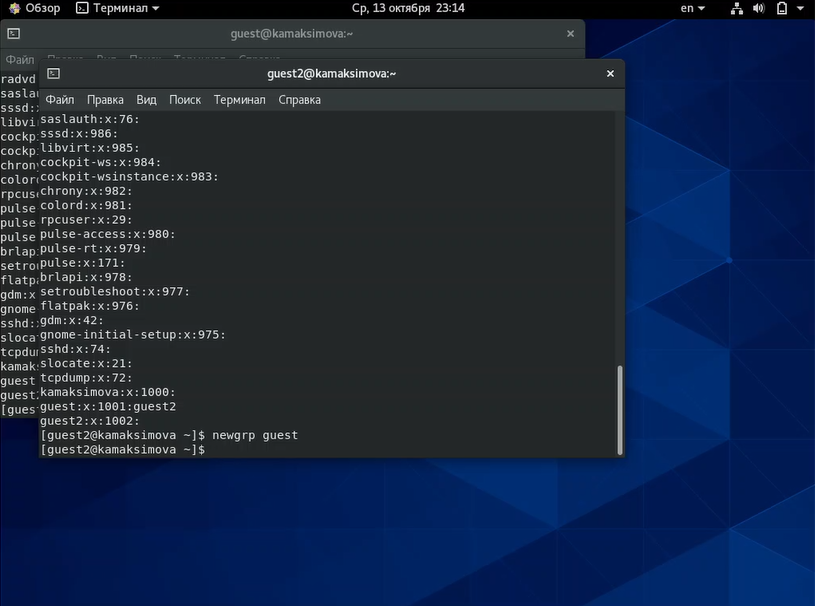


Рис 14. Регистрация пользователя guest2

[Рисунок 14](image/14.png)

От имени пользователя guest изменим права директории “/home/guest”,разрешив все действия для пользователей группы

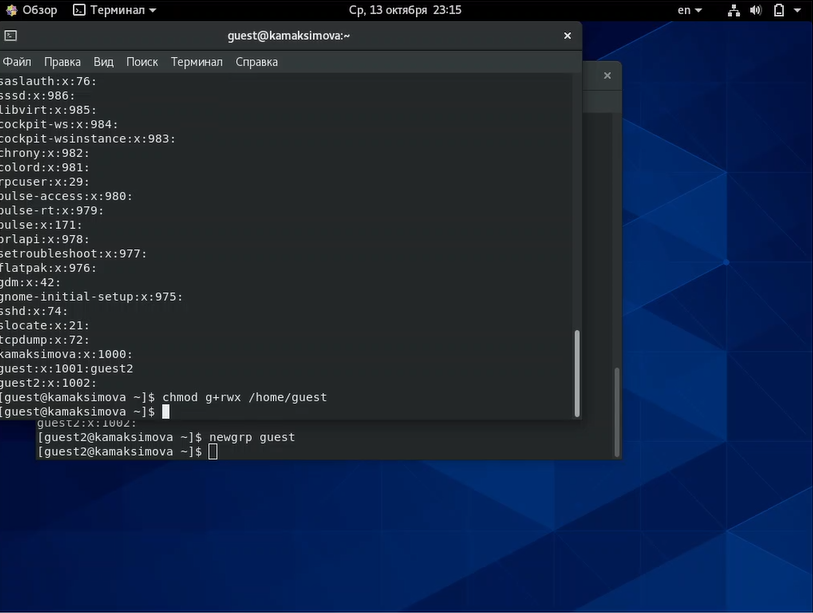


Рис 15. Изменение прав директории

[Рисунок 15](image/15.png)

От имени пользователя guest снимаем с директории “/home/guest/dir1” все атрибуты

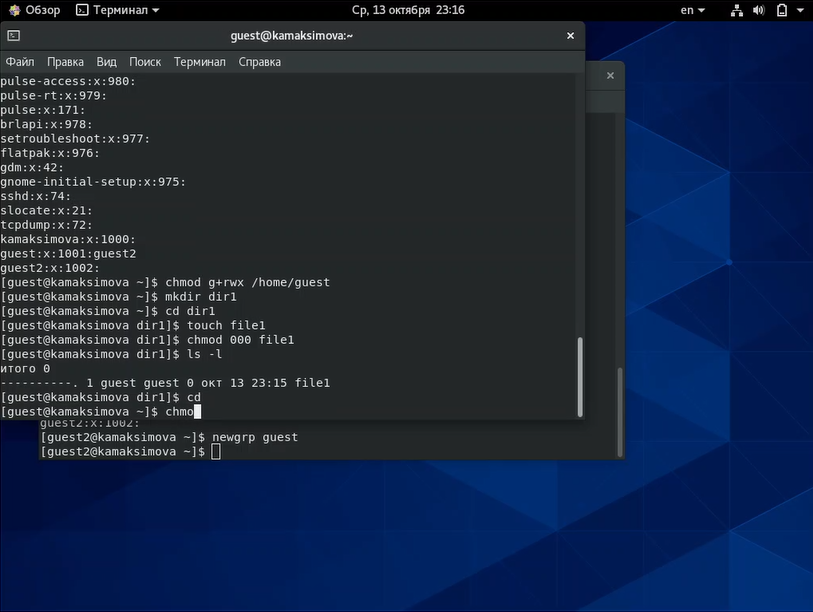


Рис 16. Снимаем все права

[Рисунок 16](image/16.png)

Меняя атрибуты у директории dir1 и файла file1 от имени пользователя guest и делая проверку от пользователя guest2, заполнила таблицу “Разрешенные права и действия для пользователей групп” определив опытным путём, какие операции разрешены, а какие нет.

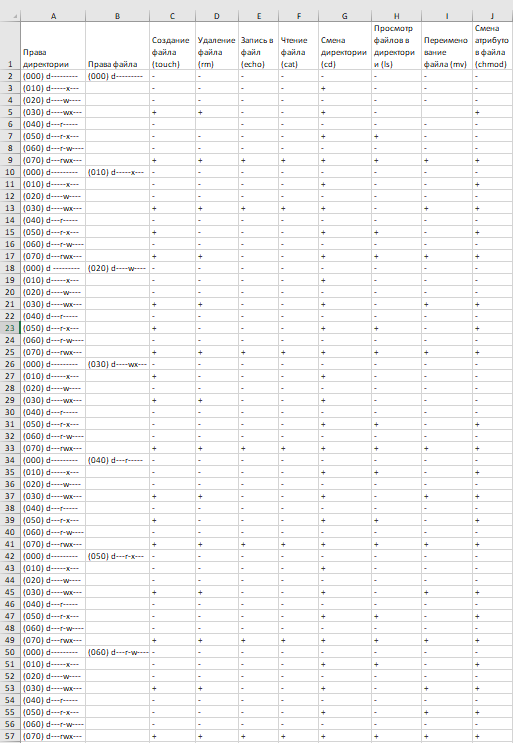


Рис 17. Таблица “Разрешенные права и действия для пользователей групп”

[Рисунок 17](image/17.png)

На основании заполненной таблицы определила те или иные минимально необходимые права для выполнения пользователем guest2 операций внутри директории dir1

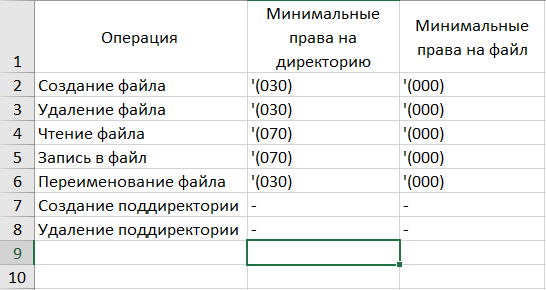


Рис 18. Таблица “Минимальные права для совершения операций”

[Рисунок 18](image/18.png)

# Выводы

В ходе лабораторной работы были установлены разрешенные действия для файла и директории для пользователей групп, а так же были установлены минимально необходимые права для совершения тех или иных действий.

# Список литературы

[1. Права доступа к файлам в Linux](https://losst.ru/prava-dostupa-k-fajlam-v-linux)

[2. Терминал Linux](https://linuxrussia.com/terminal-chmod-chown.html)

[3. Разграничение прав доступа](https://moodle.kstu.ru/pluginfile.php/318215/mod_resource/content/1/Теория_разграничение_прав_пользователи.pdf)